1 Point of Contact Information

Name	Title	Date Reported to IRT
Division/Organization	Building/Room	Email
Office Telephone:	Cell Telephone:	

2 IC Incident Contact Information

[This form applies to all users of information technology (IT) resources used in support of National Institutes of Health (NIH) whether owned, installed, maintained or operated by the IC, at remote locations, or at a contractor or research facility operating under a grant or contract with the IC.]

Incident Report Number:	Report Name	
If primary network/system administrator is not an IC employee or permanent on-site contractor, provide POC information.		
Name	Title	Email
Office Telephone:	Cell Telephone:	
If the primary systems administrator is someone other than you, provide POC information.		
Name	Title	Email
Office Telephone:	Cell Telephone:	

3 Incident Assessment Information

3.1 Physical location of the computer system(s)/network(s)

Address:	Build/Room:

3.2 Date/ Time and duration of incident (Be as specific as possible)

Date & Time:	Duration:

3.3 Affected system / network & IC Mission Critical

IP Address	Critical (Y or N)	System Name/Function (e.g., Web or FTP server)	Date & Time last modified/updated	Date & Time last scanned

Was the system modified or tampered with in any way since the incident was identified (Yes/No):

3.4 Nature of Problem (Check all that apply and indicate number of affected system if known):

Unauthorized Privileged Access		Denial of Resources (DoD or DDoS)		Theft (Date/Software)	
Unauthorized User Access		Resource Impairment		Theft (Equipment)	
Unauthorized File Modification		Probes or Scans		Sniffing	
Vandalism (e.g., web defacement)		Unknown (explain):			

Has the problem been experienced before (Yes or No):

If yes, explain:

3.5. Suspected method of intrusion or attack (List the number of affected system, if known)

Vulnerability Exploit		Distributed Denial of Service		Trojan Exploit		Logic Bomb	
Virus (name if known)		Denial of Service		Trap Door Exploit		Malware	

Has the problem been experienced before (Yes or No):

If yes, explain:

3.6. Suspected perpetrator(s) and possible motivation(s) for the attack:

Insider/Disgruntled Insider		Partnering Agency		Inexperienced Hacker	
Foreign Individual or Group		Former Employee		Experienced Hacker	

Other (explain):

3.7 What was the apparent source (IP Address/Domain/ISP) of the attack?

3.8 Was there any evidence of spoofing?

3.9 What tools did you use to build your analysis:

3.10 List any relevant logs or proof of system compromise:

3.11 What operating system/application types and versions were affected (List number of affected systems if known):

Unix (Vendor?)		Web Application (Vendor?)		Database Application (Vendor?)		DNS	
Linux (Vendor)?		Win95/98/NT/2K/XP		Custom Application (Vendor?)		Unknown	
Macintosh		Novell		Electronic Mail (Vendor?)			

Other (explain):

3.12 Class and Number of Machines Affected

Firewall/Gateway/Network Load Balancer		Intrusion Detection Server/Sensors		Workstation/Laptop	
Content Filter Devices		Printers and Peripherals		Unknown	

Other (explain):

3.13 What protective security measures were in place?							
Firewall Rulesets		Security Auditing Tools		Incident/Emergency Response Team		Encryption	
Packet Filtering		Access Control Lists		Authentication Application		Intrusion Detection	
Banners		File Integrity Checking		Secure Remote Access Protocols		Unknown	
Other (explain):							

3.14 Did the intrusion/attack result in a loss/compromise of sensitive or proprietary information (e.g., stolen password files)?

3.15 Did the intrusion/attack result in damage to systems or data?

3.16 What actions and/or technical mitigations have been performed:					
System disconnected from the network		Log files moved to remote systems and analyzed		Systems scanned in depth for introduced vulnerabilities	
Systems reloaded from original installation media		System binary CRCs Validated		Systems scanned for Trojan programs or “Root Kits”	
Systems restored from backups taken prior to attack		System binary file permissions validated		Systems swept for viruses and/or worms	
Other (Explain Below):					

3.17 If any of the actions and/or technical mitigations are “temporary” when will they be removed?

4 Notification Information

NIH Incident Response Team (IRT) [301-881-9726]	IRT@NIH.GOV
CERT Federal Computer Incident Response Center:	http://www.fedcirc.gov/
[412-268-6321 (Hot Line), 1-888-282-0870 (Toll Free), 1-412-268-6989 (FAX)]	
National Infrastructure Protection Center (NIPC):	www.nipc.gov/incident/incident.htm
NIH Incident Response Procedures:	http://irm.cit.nih.gov/irtonly/ir_procedures.html
NIH ISSO Contact Information:	http://irm.cit.nih.gov/nihsecurity/scroster.html
IC Computer Security Staff:	https://130.14.15.184/contactlist.htm

Individuals Notified of the Security Incident	Yes?	If Yes, who was notified?
IC Computer Security Staff, IT Director, and Organizational Director		
Any organization outside of the IC (e.g., NRC, NavyMed, NIHFCU)		
Security Representatives for each of the IC organizations		
Other organizations (e.g., CERT, FedCIRC)		
IC Physical Security Department (e.g., NIH Police, Building Security)		
Local, State, or Federal Law Enforcement Agency		

5 Lessons Learned

5.1 Note corrective, procedural and technical changes that might help to prevent this type of event in the future.		
5.2 Date Incident Closed:	**IRT Personnel:**	**Email:**